CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

2. (U//FOUO) The BULLRUN data label (for use in databases) and marking (for use in hard- or softcopy documents) are for internal NSA/CSS use only. It will appear in the classification line and corresponding portion markings after all applicable ODNI-approved markings are in place. The format is:
Classification//SCI Control System Markings//CAPCO-approved Dissemination Control Markings/BULLRUN. Examples include:

- TOP SECRET//SI//REL TO USA, FVEY/BULLRUN
- TOP SECRET//SI-ECI PIQ//ORCON/NOFORN/BULLRUN

3. (U//FOUO) Appendix A lists specific BULLRUN capabilities. Details may be protected by one or more ECI. Contact CES CAO for access to the appendix or further guidance.

Description of Information	Classification/Markings	Reason	Declass	Remarks
A. (U) General				
A.1. (U) The coverterm BULLRUN standing alone	UNCLASSIFIED	N/A	N/A	
A.2. (U//FOUO) The coverterm BULLRUN in association with	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	(U//FOUO) Related ECIs include, but are not limited to:

Description of Information	Classification/Markings	Reason	Declass	Remarks
NSA/CSS, SIGINT, IC, or any of the related ECIs				APERIODIC, AMBULANT, AUNTIE, PAINTEDEAGLE, PAWLEYS, PITCHFORD, PENDLETON, PICARESQUE, PIEDMONT
B. (U) Partnering/Collaboration				
B.1. (U) The fact that Cryptanalysis and Exploitation Services (CES) works with: • NSA/CSS Commercial Solutions Center (NCSC) • Tailored Access Operations (TAO) • Second Party partners	UNCLASSIFIED	N/A	N/A	
B.2. (U//FOUO) The fact that Cryptanalysis and Exploitation Services (CES) works with: • NSA/CSS Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with specific industry partners • Tailored Access Operations (TAO) to leverage specific computer network exploitation activities • specific U.S. Government/IC entities to further NSA/CSS capabilities against encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
B.3. (TS//SI//REL) Details of the CES collaboration with: • NSA/CSS Commercial Solutions Center (NCSC) to leverage sensitive, cooperative relationships with industry partners • Tailored Access Operations (TAO) to leverage computer network exploitation activities • Second Party partners • specific U.S. Government/IC entities to further NSA/CSS capabilities against encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.

Description of Information	Classification/Markings	Reason	Declass	Remarks
C. (U) Capabilities & Targeting				
C.1. (U//FOUO) The fact that Cryptanalysis and Exploitation Services (CES) develops cryptanalytic capabilities to exploit the inherent vulnerabilities in the encryption used in unspecified network communication technologies	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	
C.2. (U//FOUO) The fact that NSA/CSS targets specific encrypted network communication technologies	SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may raise classification level and may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.3. (TS//SI//REL) The fact that NSA/CSS has some capabilities against the encryption in TLS/SSL, HTTPS, SSH, VPNs, VoIP, WEBMAIL, and other network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.4. (U//FOUO) The fact that NSA/CSS has a capability against the encryption used in a specific implementation of a network communication technology	TOP SECRET//SI// REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Specific implementations may be identified by specifying equipment manufacturer, service provider or target implementation. (U//FOUO) Details may be protected by one or more ECIs

Description of Information	Classification/Markings	Reason	Declass	Remarks
				and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.5. (U//FOUO) Details revealing specific sources and methods that enable a capability against the encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
C.6. (TS//SI//REL TO USA, FVEY) The fact that NSA/CSS develops implants to enable a capability against the encryption used in network communication technologies	TOP SECRET//SI// REL TO USA, FVEY See Remarks.	1.4 (c)	25 years*	(U//FOUO) Details will be protected by one or more ECIs. Contact CES CAO for further guidance.
D. (U) Processing & Handling				
D.1. (U//FOUO) Decrypts (aka plaintext) obtained from BULLRUN capabilities	TOP SECRET//SI// REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c)	25 years*	(U//FOUO) Decrypts or any data extracted from the decrypts must be handled within the secure BULLRUN COI and must be marked with the BULLRUN data label, unless Chief S31 (or designee) has approved handling or dissemination outside of BULLRUN. Reports generated from BULLRUN-derived information must not reveal BULLRUN details. (U//FOUO) Details may be

Description of Information	Classification/Markings	Reason	Declass	Remarks
				protected by one or more ECIs. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.
D.2. (U//FOUO) Cryptographic information obtained from BULLRUN capabilities	TOP SECRET//SI// REL TO USA, FVEY/ BULLRUN at a minimum See Remarks.	1.4 (c)	25 years*	(U) Examples include algorithm parameters and passwords. (U//FOUO) Details may be protected by one or more ECIs and/or the secure BULLRUN COI. In addition, details may need to be marked with the BULLRUN data label. (U//FOUO) See paragraph #2 at the beginning of this guide for details on how to mark BULLRUN information. (U//FOUO) Appendix A lists specific BULLRUN capabilities. (U) Contact CES CAO for further information.

(U) 25 years*: Declassification in 25 years indicates that the information is classified for 25 years from the date a document is created or 25 years from the date of this original classification decision, whichever is later.

(U) ACRONYMS/DEFINITIONS:

(U) **Capabilities** – For the purposes of this classification guide, the NSA/CSS ability to exploit a specific technology. This may encompass acquiring and processing plaintext data and/or acquiring, decrypting and processing encrypted data.

(U) **HTTPS –** HTTP traffic secured inside an SSL/TLS session, indicated by the https:// URL, commonly using TCP port 443

(U) **IPSEC -- IPSec**, or **IP Security**, is the Internet Engineering Task Force (IETF) standard for layer 3 real-time communication security. IPSec allows two hosts (or two gateways) to establish a secure connection, sometimes called a tunnel. All traffic is protected at the network layer. (IETF is the Internet Engineering Task Force, a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications.)

(U) **PPTP – Point-to-Point Tunneling Protocol** is a method for implementing virtual private networks. The PPTP specification does not describe encryption or authentication features and relies on the protocol being tunneled to implement security functionality.

(U) **SSH – Secure Shell.** A common protocol used for secure remote computer access

(U) **SSL – Secure Sockets Layer.** Commonly used to provide secure network communication. Widely used on the internet to provide secure web browsing, webmail, instant messaging, electronic commerce, etc.

(U) **TLS – Transport Layer Security.** The follow-on to SSL, SSLv3 and TLSv1.0 are nearly identical.

(U) **VoIP – Voice over Internet Protocol.** A general term for the using IP networks to make voice phone calls. The application layer protocol can be standards-based (e.g., H.323, SIP), or proprietary (e.g., Skype).

(U) **VPN – Virtual Private Network.** A private network that makes use of the public telecommunications infrastructure, maintaining privacy via the use of a tunneling protocol and security procedures that typically include encryption. Common protocols include IPSEC and PPTP.